Asociación Española del Transporte

Resumen Ejecutivo

Introducción y comparativa de diferentes tecnologías de registro distribuido para el desarrollo de casos de uso

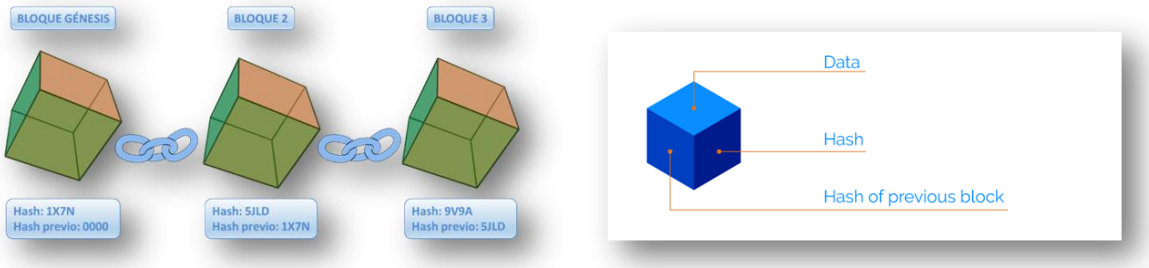
1 INTRODUCCIÓN

La tecnología Blockchain, en boga desde la aparición del Bitcoin ha evidenciado, desde entonces, numerosos casos de uso sin que, en muchos casos, se haya pasado con éxito la fase de "Prueba de Concepto". Por este motivo, la aproximación de muchos usuarios hacia esta tecnología es incompleta. El **objetivo de este estudio es ilustrar el estado del arte** de estas tecnologías, analizando sus pros y contras, aportando un análisis de posicionamiento y una comparativa entre ellas, cara a posibilitar la toma de decisión de profesionales y compañías que estén planteando su utilización.

Se ha decidido orientar el estudio hacia soluciones útiles para el desarrollo de casos de uso reales para el sector transporte y logística, ya que es el segundo con mayor porcentaje de aplicación de la tecnología Blockchain, solo por detrás del Fintech, y es el escenario perfecto para su aplicación, con entornos complejos, colaborativos, muchos actores, conflictos de intereses, documentación estandarizada y fuerte normativa.

2 ESTADO DEL ARTE

Se denomina **Blockchain** a un conjunto de registros (bloques) enlazados unos con otros (cadena) formando un conjunto cifrado de datos que se despliega sobre una red descentralizada. La información contenida en los bloques se codifica ("hash"). Los bloques contienen su propia información útil, así como el código hash del bloque anterior. Tanto la información útil de un bloque como el código hash del bloque precedente se utiliza para generar su propio hash.



Por definición, los bloques están necesariamente ligados entre sí (encadenados): cualquier variación en uno de los bloques rompería la integridad de la estructura, volviéndose inconsistente. La información que almacenan es inalterable e inmutable.

Existen fundamentalmente tres tipos de cadenas de bloques:

- **Públicas**. Formadas por nodos de usuarios que, voluntariamente y sin restricciones, entran a formar parte de la red a través de la instalación del servicio en su nodo. Este modelo totalmente descentralizado es en el que se basan Bitcoin o Ethereum.

- **Privadas**. Desarrolladas para un propósito concreto, siendo que el administrador distribuye y asigna los nodos, conociendo identidades y claves de los usuarios. Típicamente empleadas por organizaciones para el desarrollo de casos de uso, donde un usuario entra como cliente. No son totalmente descentralizadas ni cumplen todos los requisitos de las cadenas de bloques, aunque sí se puede garantizar un mínimo nivel de servicio y sus parámetros son totalmente configurables.

- **Permisionadas**. Se trata de un híbrido de las anteriores, en el que los usuarios solicitan permiso para entrar en la red, identificándose y aportando sus nodos. La red queda formada por el conjunto de nodos, distribuyéndose el consenso y el esfuerzo entre los usuarios. El enfoque es descentralizado, si bien existe un agente detrás al que contactar en caso de incidencia.

Resumen

	GOBERNANZA	ACCESO	OBJETIVO	NIVEL DE SERVICIO	EJEMPLO
PÚBLICAS	Descentralizada	Cualquiera	Criptomonedas	No	Bitcoin
PRIVADAS	Centralizada	Solo clientes	Casos de uso	Si	Tradelens
PERMISIONADAS	Descentralizada	Bajo autorización	Casos de uso	Parcial	Alastria

Para poder generar bloques válidos dentro de una cadena se requiere la incorporación de algoritmos de consenso. Constan de diferentes procesos de generación y corroboración, mediante diversos mecanismos, de la integridad de los bloques. Son elementos necesarios para garantizar las características fundacionales de las cadenas de bloques: inmutabilidad, veracidad y seguridad de la información. Se tienen los siguientes algoritmos:

- **Proof of Work (PoW)**. Algoritmo primigenio de Blockchain, muy arraigado en el mundo Fintech. Está enfocado a aplicaciones de minería de datos y redes de criptomonedas. El protocolo establece condiciones para dar por válido un bloque, con base en unas entradas y unas salidas.

- **Proof of Stake (PoS)**. Al igual que el anterior, goza de bastante raigambre en el universo Blockchain en aplicaciones de criptomonedas. La validación de un bloque la llevan a cabo un conjunto de nodos seleccionados de forma aleatoria, en función del cumplimiento de un conjunto de requisitos.

- **Proof of Authority (PoA)**. Difiere de los anteriores, siendo su enfoque el desarrollo de casos de uso en redes privadas o permisionadas. Para generar nuevos bloques se elige de mantera aleatoria varios nodos validadores de una lista prestablecida. La validación del nuevo bloque se realiza mediante voto por mayoría, considerando los nodos que no están en esta lista, siendo esta mayoría configurable.

Resumen

ALGORITMO	ENFOQUE	SEGURIDAD	FINALIDAD	CONSUMO
Proof of Work	Criptomonedas	Media	No	Alto
Proof of Stake	Casos de uso	Media	Si	Bajo
Proof of Authority	Casos de uso	Media	A elegir	Bajo

3 COMPARATIVA

En los siguientes apartados se desarrolla una comparativa de diversas redes y clientes Blockchain, considerando los siguientes parámetros:

- Nivel de madurez (grado de desarrollo y tiempo de la solución en producción).
- Tipo de red (pública, privada o permisionada).
- Disponibilidad de token (cuenta o no la red con criptodivisa o criptoactivo propio).
- Algoritmo de consenso empleado.
- Soporta o no lenguaje *Smart Contracts*.
- Regulación de datos (cumplimiento con estándar internacional).
- Orientación principal de la red (por parte de los usuarios).
- Flexibilidad (posibilidad de parametrizar con afecciones limitadas).
- Interoperabilidad (posibilidad de conectarse a otras redes/clientes).
- Escalabilidad (incremento del nº de bloques y de transacciones).
- Tiempo (de generación) por bloque.
- Actividad (histórico).
- Disponibilidad de entorno de *testing*.

Los resultados de la comparativa se muestran a continuación, en formato tabular.

BLOCKCHAIN	Nivel de madurez	Tipo de red	Dispone de token	Consenso	Smart Contracts	Lenguaje Smart Contracts	Regulación de datos	Orientación principal de la red	Flexibilidad	Interoperabilidad	Escalabilidad	Tiempo por bloque	Actividad	Testing
Bitcoin	Alto	Pública	Sí	PoW	No	No	No	Transacciones y valor monetario	No	No	No	10min	Alta	No
ZCash	Alto	Pública	Sí	PoW	No	No	GDPR GLBA AML	Transacciones y valor monetario	No	No	Parcialmente	2.5 min	Alta	No
Ethereum	Alto	Pública	Sí	PoW, PoS	Sí	Solidity	No	Transacciones y valor monetario	No	No	Parcialmente	20s	Alta	Sí
Ripple	Bajo	Privada	Sí	BFT	No	No	No	Transacciones y valor monetario	No	No	Parcialmente	2.5 min	Media	No
Hyperledger Fabric	Alto	Privada	No	A elegir PoW, PoA	Sí	Java, Golang	GDPR HIPAA	Dirigida a empresa	Sí	Parcialmente	Sí	A elegir (1s)	Media	No
Corda	Bajo	Privada	No	State	Sí	Java, Kotlin	HIPAA HER EMR	Dirigida a empresa y finanzas	Sí	No	No	1s	Media	Sí
Hyperledger Sawtooth (Intel)	Bajo	Privada	No	PoET	Sí	A elegir	No	Dirigida a empresa	Sí	Parcialmente	Sí	10s	Baja	No
Quorum	Medio	Privada	Sí	IBTF	Sí	Solidity	Parcialmente	Dirigida a empresa y finanzas	Parcialmente	Sí	Parcialmente	A elegir (2s)	Alta	No
Hashgraph	Muy bajo	Privada	Sí	Gossip	Sí	Solidity	KYC AML	Dirigida a empresa	Parcialmente	Parcialmente	Sí	5s	Media	No
IOTA	Medio	Privada	Sí	PoW	No	No	Parcialmente	Intercambio de información en IoT	Parcialmente	Parcialmente	Sí	No	Baja	No
EOS	Bajo	Pública	Sí	DPoS	Sí	C++	No	Transacciones y valor monetario	Sí	No	Parcialmente	0.5s	Baja	No
Insolar	Muy bajo	Permisionada	Sí	Globula Consensus	Sí	Java, Golang	GDPR HER HIPAA EMR	Dirigida a empresa	Sí	Parcialmente	Sí	10s	Media	No
VeChain	Muy bajo	Pública	Sí	PoA	Sí	Solidity	GDPR China	Integración de empresas	Sí	No	Parcialmente	10s	Baja	No
Alastria (Red T/B)	Medio	Permisionada	Sí	PoA	Sí	Solidity	GPDR LSSI AML	Dirigida a empresa	Parcialmente	Parcialmente	Parcialmente	2s	Media	Sí
Hyperledger Besu	Medio	Privada	Sí	A elegir Pow, PoA	Sí	Solidity	GDPR HIPAA	Casos de uso y Dapps	Sí	Sí	Sí	A elegir	Alta	Sí

4 CONCLUSIONES

De entre las opciones anteriormente analizadas, en este estudio destacamos: Hyperledger Besu, Hyperledger Fabrica y Quorum:

La alternativa Besu alberga características tanto de Hyperledger como de Quorum y responde bien al interrogante de cómo interoperar diferentes redes distribuidas, ya que es la primera que es realmente interoperable. Besu mejora a Quorum en cuanto a características técnicas y operacionales: mejor latencia, mayor capacidad de transacciones, menor tiempo de respuesta, mayor disponibilidad, *Smart Contracts* de permisionado y desarrollo de aplicaciones descentralizadas dentro de la propia red, creando un ecosistema de más valor para el desarrollo, tanto de casos de uso, como de aplicaciones. En cuanto a arquitectura, Fabric presenta una arquitectura compleja, no exenta de problemas, especialmente de gobernanza y de escalado. Por su parte, la arquitectura de Besu es muy similar a la de Quorum, de carácter descentralizado.

Diferentes consorcios nacionales e internacionales, como *European Blockchain Services Infrastructure* (EBSI) en Europa, LacChain en Latinoamérica y Alastria en el ámbito nacional, han apostado por Besu para el despliegue de sus redes Blockchain.

También está siendo implementada en varias plataformas referentes, nacionales y europeas, del sector **transporte y logística**, donde antes Quorum y Fabric eran las opciones predeterminadas, especialmente teniendo a **Tradelens**, solución desarrollada por IBM y Maersk en torno a Fabric sobre 2018, o **SIMPLE** como precursores.

Pero con el paso de los años, se han visto debilidades en estas dos alternativas que **Besu** es capaz de subsanar.

Trazabilidad extremo a extremo de la cadena de suministros, automatización y certificación de información son algunas de las funcionalidades más demandadas, en donde Besu sobresale.

Generalizando, se puede decir que Besu, que alberga las ventajas de Hyperledger y Etherum, es una de las tecnologías más punteras y ha crecido de manera considerable desde hace meses a esta fecha, debido a que los desarrolladores han visto beneficiosas características.

5 CRÉDITOS

Este estudio ha sido elaborado para la AET, por:

Coordinador del Estudio:	Carlos La Fuente	SOCIO PROTECTOR	Eurotech TLS	
Asesor:	Néstor Castanedo	SOCIO PROTECTOR	Eurotech TLS	
Coordinador Grupo de Trabajo:	Jorge Aldegunde Piñeiro	Junta Directiva	Ing. Telecomunicación	
Coordinador Grupos de estudio de la AET	Juan Manuel Martínez Mourín	Vicepresidente	Ing. Telecomunicación	

Bibliografía:

- Comparativa de soluciones Blockchain (Eurotech TLS)
- Procedimiento de despliegue de una red Hyperledger Besu (Eurotech TLS)
- ¿Qué es Blockchain? Estado del arte (Eurotech TLS)
- Aplicación de Blockchain al transporte de viajeros y su potencial aplicación en MaaS (AET)
- Conceptos Blockchain #1: Cadena de bloques & Trazabilidad (Cibernos)
- Algoritmos De Consenso: La Raíz De La Tecnología Blockchain (101 Blockchains)
- https://besu.hyperledger.org/en/stable/
- https://github.com/hyperledger/besu
- https://wiki.hyperledger.org/display/BESU/Building+from+source
- https://consensys.net/quorum/
- https://www.hyperledger.org/use/fabric

Asociación
Española
del Transporte

CIF: G28901296

Calle General Arrando 38, Madrid, 28010

info@aetransporte.org

www.aetransporte.org

www.linkedin.com/company/aetransporte

@AsocEspTransp